GIDE
GIDE LOYRETTE NOUEL

TELECOMMUNICATIONS, MEDIA & TECHNOLOGY | CHINA | 10 MAY 2017

CHINA RELEASES DRAFT MEASURES FOR TRANSFER OF DATA OVERSEAS

Further to the issuance of the *Cyber Security Law* on 7 November 2016 (which will come into force on 1 June 2017), the Cyberspace Administration of China released a draft version of the *Measures for the Security Assessment of Transfers of Personal Information and Critical Data Overseas* (the "**Draft Measures**") on 11 April 2017 for public comment.

As detailed in our previous client alert (link), the *Cyber Security Law* imposes an obligation on operators of key information infrastructure to localise in China all personal information and critical data collected in China. It also subjects any transfer of such data overseas to a security assessment.

The Draft Measures would specifically regulate such security assessment, as well as broaden the obligation to localise data in China.

This Client Alert highlights the key points of the Draft Measures and their potential impact on network operators in China.

STRENGHTHENED REQUIREMENTS FOR DATA LOCALISATION

The Draft Measures require all network operators to store in China all personal information and critical data collected and generated in the course of their operations in China. This obligation goes beyond the provisions of the *Cyber Security Law*, under which the data localisation requirement applies only to operators of "key information infrastructure".

However, the Draft Measures does retain the same definitions as the *Cyber Security Law*. "Network operators" include network owners, network managers, and network service providers; while "personal information" is defined as all kinds of information recorded by electronic or other means that can be used (independently or in combination with other information) to identify the personal information of individuals, including but not limited to names, dates of birth, ID numbers, biometrics, addresses, and telephone numbers.

The Draft Measures introduce a definition for "critical data" as data closely related to national security, economic development, and public interests. The specific scope of critical data is to be further stipulated under national standards and guidelines.

SECURITY ASSESSMENT

Any transfer of personal information or critical data outside China must be necessary for business purposes and pass a security assessment. The Draft Measures create two types of security assessment: assessments carried out by network operators (self-assessment) and assessments carried out by Chinese authorities (government assessment).

Before any transfer of personal information or critical data overseas, networks operators are generally required to conduct a self-assessment and are responsible for the results of the assessment.

According to the Draft Measures, the security assessment must focus on the following aspects:

- Necessity of the overseas data transfer;
- The quantity, scope, type, and sensitivity of the data to be transferred, and for personal information, whether the concerned individual(s) have consented to such transfer;
- The data recipient's safeguard measures, capabilities, and standards for security protection, and the network security requirements of the country and region where the data recipient is located;
- Risks of the data being divulged, damaged, tampered with, or misused after being transferred abroad and any subsequent transfer;
- Potential risks for national security, public interest, and the concerned individuals' legitimate interests arising from the data transfer and data collection; and
- Other important aspects that may need to be assessed.

In addition to the self-assessment, any transfer of the following data out of China will be subject to a government assessment:

- Data involving or cumulatively involving personal information of more than 500,000 individuals;
- Data larger than 1,000 GB;
- Data containing information on nuclear facilities, chemical or biological matters, national defence, health of the population, major engineering activities, oceanic environment, and sensitive geographical information;
- Data containing network security information, e.g. system vulnerabilities and the security of key information infrastructure;
- Personal information and critical data provided by operators of key information infrastructure to overseas parties; and
- Any other situation that may affect national security and/or public interests, and the competent regulator considers that a security assessment should be required.

Under the Draft Measures, the government assessment must be completed within 60 working days.

In addition to the self-assessment and government assessment (if applicable), network operators are responsible for conducting an annual security assessment of their overseas data transfers and reporting the results to authorities. If there is any change to the data recipients or any significant change to the purpose, scope, volume, or type of transfer, the security assessment must be updated in a timely manner.

PROHIBITED OVERSEAS DATA TRANSFERS

Under the Draft Measures, data may not be transferred overseas in the following circumstances:

- Where the concerned individual has not consented to the transfer of his/her personal information, or the transfer may infringe his/her personal interests;
- Where the transfer of data creates a risk to the safety of state politics, economy, science and technology, or national defence, or may affect national security or public interests; and
- Other circumstances identified by the Cyberspace Administration of China, public security department, security department, or other governmental authority.

COMMENTS

The Draft Measures detail the security assessment process introduced by the *Cyber Security Law*. It also unexpectedly expands the scope of security assessment by imposing security assessment obligations on all network operators (and not only operators of key information infrastructure). If passed, this new provision will create additional constraints on network operators and oblige them to carefully monitor any transfer of data overseas.

Gide will closely follow the development of the Draft Measures. In the meantime, please feel free to contact us if you have any questions regarding this or any other issue.

CONTACTS

Beijing

GUO MIN
guo@gide.com

Shanghai

FAN JIANNIAN
fan@gide.com

China/Hong Kong

DAVID BOITOUT
boitout@gide.com

Paris

ANTOINE DE LA GATINAIS
gatinais@gide.com

CHARLES-HENRI LEGER
leger@gide.com

GUILLAUME ROUGIER-BRIERRE
rougier@gide.com

STÉPHANE VERNAY
vernay@gide.com

THOMAS URLACHER
urlacher@gide.com

You can also find this legal update on our website in the News & Insights section: **gide.com**

This newsletter is a free, periodical electronic publication edited by the law firm Gide Loyrette Nouel (the "Law Firm"), and published for Gide's clients and business associates. The newsletter is strictly limited to personal use by its addressees and is intended to provide non-exhaustive, general legal information. The newsletter is not intended to be and should not be construed as providing legal advice. The addressee is solely liable for any use of the information contained herein and the Law Firm shall not be held responsible for any damages, direct, indirect or otherwise, arising from the use of the information by the addressee. In accordance with the French Data Protection Act, you may request access to, rectification of, or deletion of your personal data processed by our Communications department (privacy@gide.com).

gidelawfirm.cn

BEIJING | Unit 01, Fl. 15, Tower B Parkview Green Tower - No. 9, Dong Da Qiao Road - Chaoyang District - Beijing 100020 - P.R.C. | tel. +86 10 6597 4511 | beijing@gide.com
HONG KONG | Suite 3701, Edinburgh Tower, The Landmark, 15 Queen's Road Central - Central, Hong Kong SAR - P.R.C. | tel. +852 2536 9110 | hongkong@gide.com
SHANGHAI | Suite 2008, Shui On Plaza, 333 Huai Hai Zhong Road - Shanghai 200021 - P.R.C. | tel. +86 21 5306 8899 | shanghai@gide.com
PARIS | 22, cours Albert 1er - 75008 Paris - France | tel. +33 (0)1 40 75 60 00 | info@gide.com - gide.com